DOI: 10.17747/2618-947X-2024-1-23-29

Economic security of digital ecosystem solutions in logistics

A.V. Dmitriev[1]

[1] North-Western Institute of Management – Branch of RANEPA (Saint Petersburg, Russia)

Abstract

The article discusses issues of ensuring economic security as one of the most important qualitative characteristics of logistics systems, which determines the ability to ensure the established parameters of material flows in the process of goods distribution when implementing digital systems and technologies. Contemporary risks and threats characteristic of the development of digital transport and logistics ecosystems are analysed. The key factors for ensuring economic security and their importance in logistics are examined from the point of view of ensuring operational control over compliance with established key indicators of product distribution. An interpretation of the concept of 'economic security' is given from the point of view of protecting a business entity from external and internal threats in order to increase the level of competitiveness and sustainability of business in the market. The issues of ensuring the parameters of goods distribution within the established thresholds are addressed in order to achieve the optimal functioning of the goods distribution system and to ensure the economic activity of the enterprise with all the necessary resources. Logistics systems are studied for the effective organisation and management of material flows, aimed at ensuring the reliability of operations and the implementation of the strategy of economic entities. The need to use modern digital technologies to increase the level of economic security in logistics systems and to ensure the transparency, controllability and traceability of material flows in the field of goods distribution has been demonstrated. At the same time, the very fact of digitising cargo delivery processes is considered from the perspective of the ecosystem paradigm and the platform concept. The patterns of transformation of traditional logistics operators into providers of digital logistics services are substantiated. A model of a cyber-physical ecosystem in logistics has been developed, enabling end-to-end management of business processes and data exchange in the distribution of goods.

Keywords: economic security, logistics, digital ecosystems, transport, digital technologies, digital platforms.

For citation:

Dmitriev A.V. (2024). Economic security of digital ecosystem solutions in logistics. *Strategic Decisions and Risk Management,* 15(1): 23-29. DOI: 10.17747/2618-947X-2024-1-23-29. (In Russ.)

物流领域数字生态系统解决方案的经济安全

A.V. Dmitriev[1]

[1] 北西管理学院-俄罗斯联邦总统国民经济和行政学院分校（俄罗斯，圣彼得堡）

简介

文章讨论了经济安全性作为物流系统中最重要的质量特征之一的问题，这些特征决定了在数字化系统和技术的应用过程中，物流系统在货物流动过程中实现设定的物质流参数的能力。 对运输物流服务数字生态系统发展中的现代风险和威胁进行分析。研究了在物流中确保经济安全的关键因素以及它们在确保货物流动的关键指标得到遵守方面的重要性。 给出了对"经济安全性"概念的解释，从经济主体受到内部和外部威胁的程度角度来看，以提高企业在市场上的竞争力和稳定性。讨论了在设定的门槛值范围内确保货物流动参数以实现货物传送系统的最佳运作和企业经营活动所需的所有必要资源的问题。研究了物流系统的有效组织和管理物流流程，以确保经济主体的可靠运作和战略实施。论证了在物流系统中提高经济安全水平和确保货物流动领域的透明度、可控性和追溯性的必要性，这需要使用现代数字技术。同时，将货物交付过程数字化的事实从生态系统范式和平台概念的角度进行了考察。论证了传统物流运营商转变为数字物流服务提供商的规律性。提出了一种在物流中实现端到端业务流程管理和数据交换的模型，即物理-数字生态系统模型。

关键词: 经济安全，物流，数字生态系统，运输，数字技术，数字平台。

引用文本:

Dmitriev A.V. (2024) 。 物流领域数字生态系统解决方案的经济安全性。战略决策和风险管理, 15(1): 23–29。 DOI: 10.17747/2618-947X-2024-1-23-29。(俄文)

Introduction

At present, one of the key quality features of modern transport and logistics systems is economic security, which provides control over compliance with the established parameters of material and related flows in the process of goods movement, as well as sufficient supply of enterprises with all types of resources for their economic activities.

In this case, economic security not only ensures the protection of economic entities from internal and external threats, but also stimulates the sustainable and stable functioning of entities in the context of effective counteraction to the negative impact of environmental conditions.

In this context, logistics as a science and a sphere of practical activity is aimed at the implementation of strategies of economic entities, maintaining the efficiency of their work and is connected with the optimisation of organisational and managerial efforts to promote material flows. It is obvious that in this case the absence of a well-established and effective system of economic security in the enterprise will lead to the failure of the implementation of its strategy and the risk of losing competitive advantages in the market.

In addition, the high stability and functionality of modern mechanisms for the movement of goods, including in international traffic, make it possible to increase the efficiency of all entities involved in the integrated logistics system and to optimise business processes for the delivery of goods to end users.

The purpose of this study is to substantiate the use of a methodology to ensure economic and information security in the implementation of modern digital ecosystem solutions in logistics, in the context of increasing cybersecurity threats.

1. Theoretical review

The use of digital technologies in logistics systems is now an objective and established reality. However, despite all the advantages of digitalisation, which make it possible to speed up the execution of logistics operations and track them online, digital ecosystems can be exposed to a fairly high level of external and internal threats, primarily related to the vulnerability of the information infrastructure of economic entities. Since logistics as a practical sphere of activity is closely related to the sphere of material production and delivery of products to end consumers, its sustainable functioning, including the use of modern information technologies, is one of the key factors of the state's economic security and the key to maintaining a high level of well-being of the population.

Quite a lot of scientific research is devoted to the problems of implementing digital technologies and ensuring economic security in the field of logistics and supply chain management. The authors of the work [Plotnikov et al., 2023] focus on the emergence of a wide range of new threats that give rise to the possibility of weakening national and economic security caused by turbulence and instability of the global economy, which leads to the need to strengthen the industrial potential and accelerate technological development of our country.

In the article [Malyukov et al., 2023], the authors characterise the sustainability of economic systems from the perspective of strategic content using a balanced scorecard system, which allows for the synchronicity of managing the overall efficiency of the enterprise, risks arising in the course of work, and the implementation of the economic security agenda of business systems when they operate in a wide range of modern threats and challenges.

The study [Trachuk, Linder, 2023] is devoted to the impact of digital platforms on the performance indicators of industrial enterprises in the context of creating and developing unique competitive advantages and increasing the efficiency of primary and auxiliary processes in the field of real production in order to find sources of internationalisation and enter new markets in the context of negative network effects.

The work [Nosov, 2019] substantiates the strategic role of logistics in ensuring the economic security of the country, and the effectiveness of logistics activities is defined as the basis of the economy of any state. At the same time, the methodology of logistics should be closely related to the basic tasks that ensure the comprehensive modernisation of the industrial production and technological base to neutralise external and internal threats in the economy, including in the transport and logistics sector.

2. Research material and methods

In today's conditions, the use of digital innovations and modern information technologies in the field of goods transport, ensuring online transparency and controllability of all types of flows, including material, information and financial, contributes to increasing the level of economic security in the field of transport and logistics services.

The generally accepted methods used in logistics for a long time assumed that economic benefits were only generated by the functioning of the company itself, its supply chain and its immediate business environment. Now and in the foreseeable future, we will see the dominance of the digital paradigm in the provision of transport and logistics services, based on the application of the platform concept and the creation of the necessary conditions for the formation of mature ecosystems that integrate a large number of participating entities and jointly generate high indicators of added value. At the same time, a highly secure and sustainable digital logistics information infrastructure should become a key prerequisite for implementing the new methodology.

The author's view in the publication [Bag et al., 2020] follows these trends and aims to analyse the structural and transformational processes that ensure the development of network telecommunications convergence and the expansion of information and analytical spatial interaction at various levels, including regional, state and global.

The advantages of implementing and integrating digital platform solutions in the transport logistics of a single country, as well as digital integrated platforms with global coverage, achieved by overcoming time and space gaps and barriers in the interaction of subjects of transport and logistics processes, are noted. In this context, a number of scientific studies, such as 'The State as a Platform', carried out by the

Fig. 1. Economic security factors in logistics

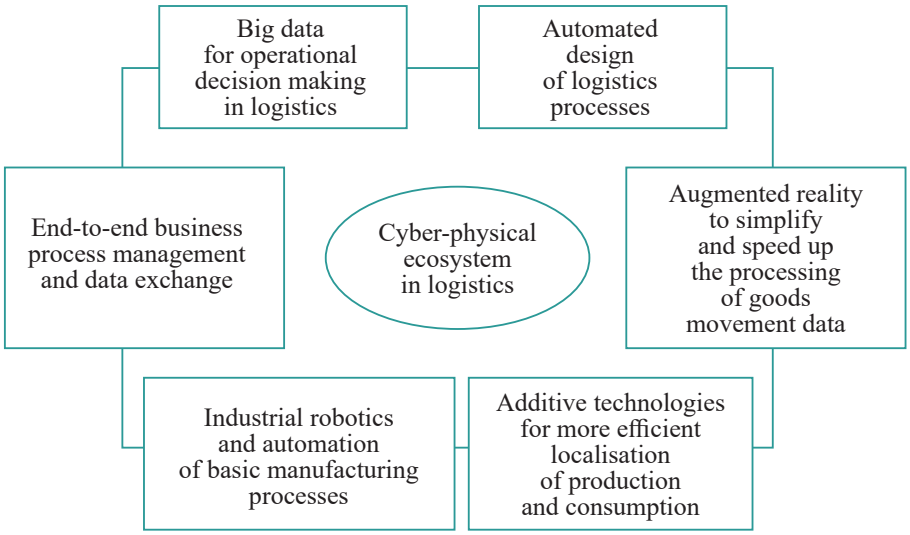
Factors	Meaning
– Well established and streamlined rules and procedures for managing logistics business processes	– Ensuring operational control over compliance with established key indicators of product movement
– Documented internal policies and accountability for compliance	– Reducing the risk of illegal actions by officials
– Compliance with workplace safety regulations	– Increasing labour productivity, reduce disruption to work schedules
– Pre-litigation handling of claims	– Reducing the number of complaints and fines
– Working with unified, standardised technologies	– Using of uniform forms of documentation and technological solutions by all subjects of the supply chain
– Use of specialised closed digital networks for data exchange	– Preventing unauthorised access to information by third parties
– Confidentiality and protection and storage of trade secrets	– Countering industrial espionage and insider attacks
– Professional retraining of employees	– Strengthening the human component of economic security

Source: [Dmitriev, 2012].

Centre for Strategic Studies, consider individuals and legal entities as priority consumers of digital government services, if all connected entities have the possibility to work with universal databases, but with a differentiated level of access. At the same time, an additional synergistic effect for users of digital services can be achieved through the use of innovative methods of network coordination and control of network interaction [Bogachev, Trifonov, 2022].

It should be recognized that the goals of the future world order and its features will be directly related to the further universal and widespread implementation of digital solutions caused by the increasing modernisation of microelectronics, telecommunications and information technologies [Khalin, Chernova, 2023].

Fig. 2. Model of a cyber-physical ecosystem in logistics



Source: [Dmitriev, 2018].

In their generality, digital tools form a model of a cyber-physical ecosystem in logistics (Figure 2), allowing the creation of a set of integrated interactions in the 'consumer-supplier' systems in the functional logistics circuit to coordinate end-to-end business processes of goods movement and data exchange on deliveries, based on big data analytics on the characteristics of goods and information on the cargo owners to make informed and rapid decisions online[1].

However, it should be recognised that the process of digital transformation in general is characterised by a number of serious risks and threats, in particular the risk of data privacy breaches, the use of malicious software and imperfect regulatory frameworks.

[1] Logistics and Supply Chain Management: Textbook for Universities (2019). Edited by V.V. Shcherbakov. M., Yurait.

Table 1
Volumetric structural and market indicators by type and category of digital privacy tools

Digital data protection tools	Market share (%)	Market share (billion roubles)	Growth rate (%)
Computer network security	45	61	20
User data protection	15	20	13
Automated workstation security tools	13	18	17
Infrastructure security	12	17	32
Application package and application protection	8	11	34
Protecting user accounts	7	9	10

Source: Forecast of the development of the cybersecurity market in Russia The Russian Federation for 2022-2026 (2022). https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022–2026-godakh/.

3. Research findings and their discussion

As mentioned above, one of the forms of implementing business processes that has recently become quite widespread in logistics is a digital ecosystem organisation based on the platform concept of managing the movement of goods. This concept is a driver for the transformation of the methods of providing digital logistics services to consumers and allows for a significant increase in the level of competitiveness of companies in the market compared to the traditional approach to the activities of logistics operators.

Logistics and Supply Chain Management: Textbook for Universities (2019). Edited by V.V. Shcherbakov. M., Yurait.

Since the provision of logistics services in digital form and the development of cyber-physical systems directly depend on the level of security of the digital infrastructure of goods distribution, in this context it is advisable to dwell on the analysis and assessment of the cybersecurity market based on the results of 2021, published in 2022 by the Centre for Strategic Research Foundation. (CSR)[2].

First of all, let's consider the structural indicators for market share volumes for 2021 by categories of information security tools (Table 1). The average annual growth rate of the cybersecurity market in Russia at the end of 2021 is estimated at more than 17%.

This value exceeds the growth of global cybersecurity market indicators, which, although historically quite high due to the industrially developed countries of Western Europe and North America, are currently growing at a lower rate (on average about 11% per year) due to the maturity and saturation that has developed in recent years. At the same time, according to CSR forecasts, the Russian cybersecurity market could reach RUB 446 billion by 2026 (Figure 3).

The above results of the study by the Centre for Strategic Research 'Forecast of the Development of the Information Security Solutions Market in the Russian Federation in 2022-2026' are also interesting because recently the Russian cybersecurity market has been significantly affected by changes in the geopolitical situation. This led to a mass exodus of Western developers and vendors of integrated solutions and information security tools from Russia in the first quarter of 2022, predicting a significant restructuring of market shares in the next five years [Bashirzade, 2022].

According to the estimates of the analytical agency CSR, from 2023 to 2027 the volume indicators of the Russian cybersecurity market should grow by at least 2.5 times. At the same time, from 2023, almost the entire budget of customers for information security tools in the B2G and B2B sectors will be spent on products from Russian suppliers, which will allow this part of the market to grow from 113 billion roubles in 2021 to 446 billion roubles in 2026.

The cybersecurity market is also significantly influenced by the active position of regulators and government bodies regarding the need for import substitution (ensuring technological independence) of technical solutions related to ensuring the secure operation of critical information infrastructure facilities[3].

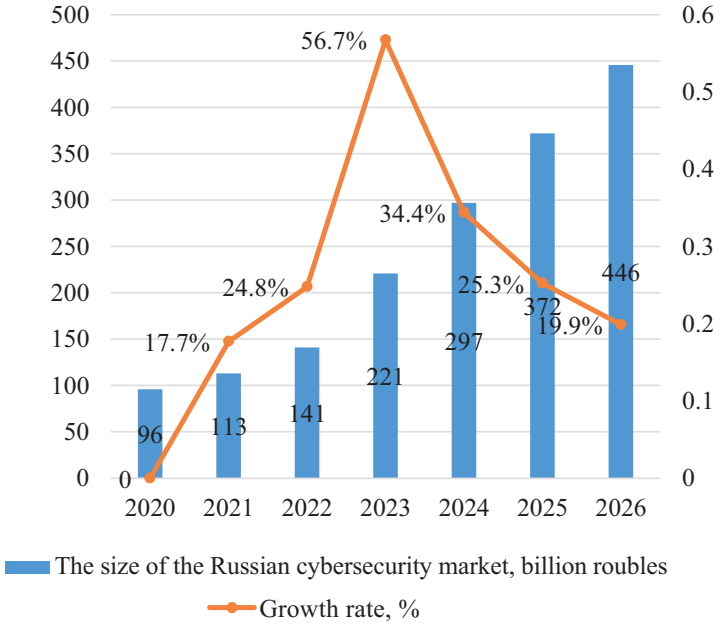
Transport logistics, on the other hand, is subject to the negative impact of a whole range of risks and threats resulting from the introduction of modern digital tools (Table 2).

According to statistics, the total number of cyber-attacks on Russia has increased by 65% since the beginning of 2023. The number of cyber-attacks on Russian services has increased 15 times. About 25,000 cyber-attacks on state digital resources were neutralised. About 1,200 cyber-attacks were directed at critical infrastructure facilities (energy, water, environmental monitoring, transport and other key systems that ensure the life of the population) [Dmitriev, Shcherbakov, 2023].

In maritime transport, the traditional systems used for safety and reporting of accidents and disasters have been replaced by fully digital local networks based on the use of

[2] The number of cyber attacks on Russian information systems has increased by 65% (2023). https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak.
[3] Forecast of the development of the cybersecurity market in the Russian Federation for 2022-2026 (2022). https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022-2026-godakh/.

Fig. 3. Dynamics and volume forecast of the cybersecurity market in Russia



Source: Forecast of the development of the cybersecurity market in the Russian Federation for 2022-2026 (2022). https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-resheniy-dlya-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii-v-2022–2026-godakh/.

cloud technologies, in particular software that controls electronic navigation. These networks have become a tempting target for hackers because they are designed to continuously collect, integrate and analyse on-board information to track a vessel's location, cargo data, technical issues and a range of navigational issues in different parts of the world's oceans and coastal waters. Rail transport is facing a similar situation. Traditional wired train control systems, which were limited in their ability to share information with the outside world, are being replaced by wireless standards that ensure the operability of wide networks linking freight and passenger trains to the station attendant's control room. And this can also be an attractive target for cyber attacks.

In order to neutralise the above risks and threats, it is necessary to increasingly implement digital ecosystems in transport logistics, whose infrastructure will include a set of modern information systems and technologies that have potential benefits for the economy and society, and also allow

Table 2
Threats to the introduction of digital tools in transport logistics

Risks of Big Data	Risks of the Industrial Internet	Artificial intelligence and robotics risks	Risks of a distributed ledger system
• Breach of data privacy • Suboptimal system for collecting and storing big data • Partial or complete loss of data due to processing errors • Big data processing does not produce results for analysts • Unwillingness to change on the part of staff and management	• Malware injection, device control interception, device destruction and theft • Software vulnerability • DDoS attacks on a computer system • System, network and device failure due to power outages and other man-made and natural factors	• Lack of machine capacity to solve problems • Displacement of labour by artificial intelligence • Errors in the training of artificial intelligence and the implementation of robotics • Vulnerability of robotics (programming, calibration, controllers) • Most people prefer human interaction	• ББlockage and loss of funds due to code vulnerability or smart contract looping • Loss of personal data • Attacks on transaction sending and receiving nodes • Gain control through dominant computing power • Lack of regulation

Source: [Dmitriev, 2018].

Table 3
Advanced digital information technologies in transport and logistics service ecosystems

Work actively	Supposed to be implemented	Перспективные
• Development of internet sales (e-commerce) • Omni-channel (working with customers through all possible channels) • Mobile access to business information systems	• Customising production for specific orders • Customer behaviour analysis and forecasting • Digital design and modelling	• Using blockchain technology to protect information • Using cryptocurrency for peer-to-peer payments • Implementing the Internet of Things for automated production management • Artificial intelligence for automated decision making

Source: [Chernysheva et al., 2021].

for a significant increase in the efficiency of business processes in transport logistics (Table 3).

The digital information technologies from Table 3 used in transport logistics ecosystems provide access to a number of control and monitoring indicators:

– Reporting of abnormal events;
– Monitoring the temperature of perishable goods;
– Ensuring the operation of sensors and detectors;
– determining travel time, possible delays, duration of stops and date of arrival at destination;
– Determining the location of transport, navigation and routing;
– calculating the time of loading and unloading operations [Shabaeva, Shabaev, 2023].

Conclusion

Therefore, in order to eliminate the problematic issues related to the security of ecosystem solutions in logistics and supply chain management, it is necessary to use digital information services that have the following advantages [Dmitriev, Shcherbakov, 2023]:

– improving the efficiency of logistics business processes related to the movement and delivery of shipments;
– meeting the urgency requirements of current shipments and integrated planning of subsequent shipments;
– reducing the rate of damaged or stolen goods during the movement process;
– quick reaction to abnormal events and situations;
– monitoring the condition of goods during transport and monitoring consignments[4].

The development of the Russian information and ecosystem security market in the context of neutralising the threats posed by the introduction of digital tools in transport and logistics systems is the key to maintaining the country's technological sovereignty. In the context of the ongoing digitalisation of all sectors of the economy, in particular industry and the transport and logistics complex, it is the strengthening of information security that will ensure control over sovereign digital assets and systems for managing the flow of goods [Plotnikov, 2023]. At the same time, since the share of foreign digital solutions in Russia will be quite high by 2022, this has made it possible to set high requirements for products from Russian manufacturers.

The process of import substitution of information security solutions, which began before 2022, is progressing at a fairly high pace, but it needs to be accelerated not only in terms of transition to Russian software, but also in terms of developing an information infrastructure built on a domestic material, technical and technological base.

References

Bashirzade R.R. (2022). Theoretical and methodological provisions for ensuring the economic security of logistics systems in the context of digitalization of the economy. *Bulletin of OrelGIET*, 1(59): 20-25. DOI: 10.36683/2076-5347-2022-1-59-20-25. (In Russ.)

Bogachev Yu.S., Trifonov P.V. (2022). A single digital space for the efficient functioning of industry. *Strategic Decisions and Risk Management*, 13(4): 376-383. https://doi.org/10.17747/2618-947X-2022-4-376-383. (In Russ.)

Dmitriev A.V. (2012). Methodological foundations of logistics management of transport and warehouse centers. *News of the St. Petersburg University of Economics and Finance*, 6(78): 76-81. (In Russ.)

Dmitriev A.V. (2018). *Digitalization of transport logistics*. St. Petersburg, St. Petersburg State Economic University. (In Russ.)

Dmitriev A.V., Shcherbakov V.V. (2023). Ensuring economic security and sustainability of supply chains in the context of digitalization. *Bulletin of the Faculty of Management of St. Petersburg State Economic University*, 15: 11-18. (In Russ.)

[4] Information security in logistics and transport (2024). https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BB%D0%BE%D0%B3%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B5_%D0%B8_%D0%BD%D0%B0_%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%B5.

Malyukov Yu.A., Nedosekin A.O., Abdulaeva Z.I. (2023). Strategic management of the economic sustainability of an enterprise in the fuzzy logic paradigm. *Strategic Decisions and Risk Management*, 14(2): 136-149. https://doi.org/10.17747/2618-947X-2023-2-136-149. (In Russ.)

Nosov A.L. (2019). Logistics in the economic security system of Russia. *Innovative Economic Development*, 5-2(53): 228-232. (In Russ.)

Plotnikov V.A., Pogodina V.V., Smirnov A.A. (2023). National economic security and state policy for industrial development. *Management Consulting*, 9: 35-44. https://doi.org/10.22394/1726-1139-2023-9-35-44. (In Russ.)

Trachuk A.V., Linder N.V. (2023). The effects of digital platforms for industrial companies: An empirical analysis under conditions of external sanctions pressure. *Strategic Decisions and Risk Management*, 14(2): 150-163. https://doi.org/10.17747/2618-947X-2023-2-150-163. (In Russ.)

Khalin V.G., Chernova G.V. (2023). Digitalization and cyber risks. *Management Consulting*, 7: 28-41. https://doi.org/10.22394/1726-1139-2023-7-28-41. (In Russ.)

Chernysheva G.N., Lavrenova G.A., Savich Yu.A., Lubyanskaya E.B. (2021). Ensuring economic security in the logistics of state defense orders. *Production Organizer*, 29(3): 171-184. DOI: 10.36622/VSTU.2021.47.14.015. (In Russ.)

Shabaeva S.V., Shabaev A.I. (2023). Tools for implementing strategies in the context of digital transformation of industrial enterprises. *Management Consulting*, (10): 69-79. https://doi.org/10.22394/1726-1139-2023-10-69-79. (In Russ.)

Bag S., Dmitriev A.V., Sahu A.K., Sahu A.K. (2020). Barriers to adoption of blockchain technology in green supply chain management. *Journal of Global Operations and Strategic Sourcing*, 0027. DOI: 10.1108/JGOSS-06-2020-0027.

About the author

Alexander V. Dmitriev
Doctor of economic sciences, associate professor, head of the Department of Security, North-Western Institute of Management – Branch of Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Saint Petersburg, Russia). SPIN: 6893-9410; ORCID: 0000-0002-3083-663X; Scopus Author ID: 57208211545; Researcher ID: ABG-4878-2021.
Research interests: economic security, logistics, supply chain management methodology.
dmitriev-av@ranepa.ru

作者信息

Alexander V. Dmitriev
经济学博士，副教授，安全系主任，北西管理学院-俄罗斯联邦总统国民经济和行政学院分校（俄罗斯，圣彼得堡）。SPIN: 6893-9410; ORCID: 0000-0002-3083-663X; Scopus Author ID: 57208211545; Researcher ID: ABG-4878-2021.
科研兴趣领域：经济安全，物流，供应链管理方法论。
dmitriev-av@ranepa.ru

The article was submitted on 16.01.24; revised on 08.02.24 and accepted for publication on 20.02.24. The author read and approved the final version of the manuscript.
文章于 16.01.24 提交给编辑。文章于 08.02.24 已审稿，之后于 20.02.24 接受发表。作者已经阅读并批准了手稿的最终版本。